The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
09/26/2019

SUBJECT:
Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Xcode, tvOS, Safari, iOS, iPadOS, watchOS, Mojave, High Sierra and Sierra. The most severe of these vulnerabilities could allow for arbitrary code execution.

- Xcode is an integrated development environment for MacOS
- tvOS is an operating system for the fourth-generation Apple TV digital media player.
- Safari is a web browser available for OS X.
- iOS is a mobile operating system for mobile devices, including the iPhone, iPad, and iPod touch.
- iPadOS is the successor to iOS 12 and is a mobile operating system for iPads
- watchOS is the mobile operating system for the Apple Watch and is based on the iOS operating system.
- Mojave is a desktop and server operating system for Macintosh computers.
- High Sierra is a desktop and server operating system for Macintosh computers.
- Sierra is a desktop and server operating system for Macintosh computers.

Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Xcode versions prior to 11.0
- tvOS versions prior to 13
- Safari versions prior to 13.0.1
- Apple TV Software 7.4
- iOS versions prior to 13.1
- iPadOS versions prior to 13.1
- watchOS versions prior to 5.3.2

- macOS Mojave 10.14.6, Security Update 2019-005 High Sierra, Security Update 2019-005 Sierra

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Xcode, tvOS, Safari, iOS, iPadOS, watchOS, Mojave, High Sierra and Sierra. The most severe of these vulnerabilities could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

- A integer overflow issue in libssh2 was addressed by updating to version ld64-507.4. (CVE-2019-3855)
- Multiple arbitrary code execution vulnerabilities with code compilation in Xcode were addressed by updating to version ld64-507.4. (CVE-2019-8721, CVE-2019-8722, CVE-2019-8723, CVE-2019-8724)
- A memory corruption issue was addressed with improved state management. (CVE-2019-8738, CVE-2019-8739)
- An authentication issue was addressed with improved state management. (CVE-2019-8704)
- An inconsistent user interface issue was addressed with improved state management. (CVE-2019-8654)
- An information leakage issue was addressed with improved handling of service worker lifetime. (CVE-2019-8725)
- An information leakage issue was addressed by restricting options offered on a locked device. (CVE-2019-8775)
- An out-of-bounds read was addressed with improved input validation. (CVE-2019-8641)

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Apple to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to download, accept, or execute files from un-trusted or unknown sources.
- Remind users not to visit untrusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Apple:
https://support.apple.com/en-us/HT210588
https://support.apple.com/en-us/HT210589

https://support.apple.com/en-us/HT210590
https://support.apple.com/en-us/HT210603
https://support.apple.com/en-us/HT210604
https://support.apple.com/en-us/HT210605
https://support.apple.com/en-us/HT210609

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-3855
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8641
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8654
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8704
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8721
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8722
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8723
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8724
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8725
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8738
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8739
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8775

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

Chris Watts
Security Operations Analyst
MS Department of Information Technology Services
601-432-8201 | www.its.ms.gov

ITS Mississippi Department of Information Technology Services
3771 Eastwood Drive | Jackson, Mississippi 39211-6381

DISCLAIMER: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited